RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PDP-T09

Homomorphic Encryption: Unlocking Power of Privacy-Preserving Computation

Deepak Behal

Information Security Officer, Capital One
(CISSP,CCSP, GCSA, GMLE, AWS ML speciality, AWS & AZURE Security Certified, CCI, PMP, PMI-ACP)

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- Homomorphic Encryption (HE) Overview
- Practical implementation and real-world applications of HE
- Homomorphic Encryption Challenges & Recent Advancements
- Homomorphic Encryption Security
- Call for Action

RSAC 2025 Conference

Homomorphic Encryption (HE) Overview (Emerging Field)

Key Security Challenge with traditional encryption methods

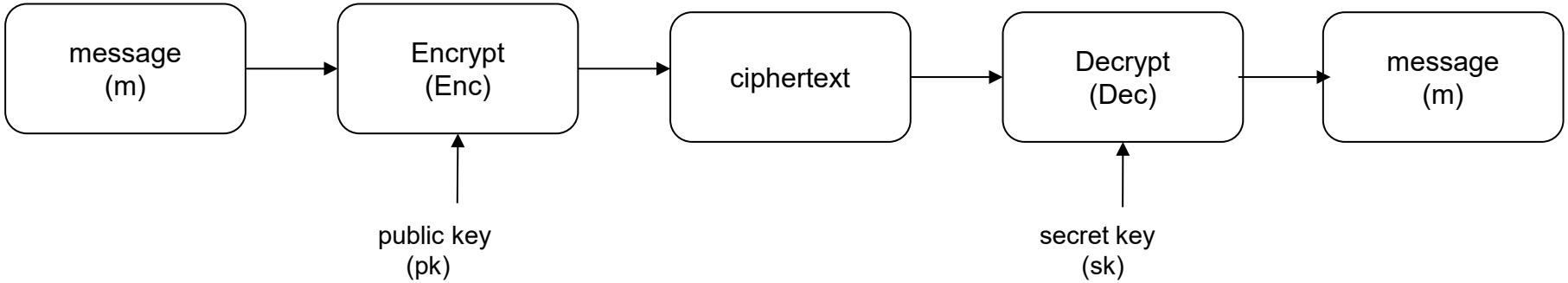
Traditional Encryption Method

- Protect Data only when it is not in Use
- Require Decryption for processing

→ Create Window of vulnerability

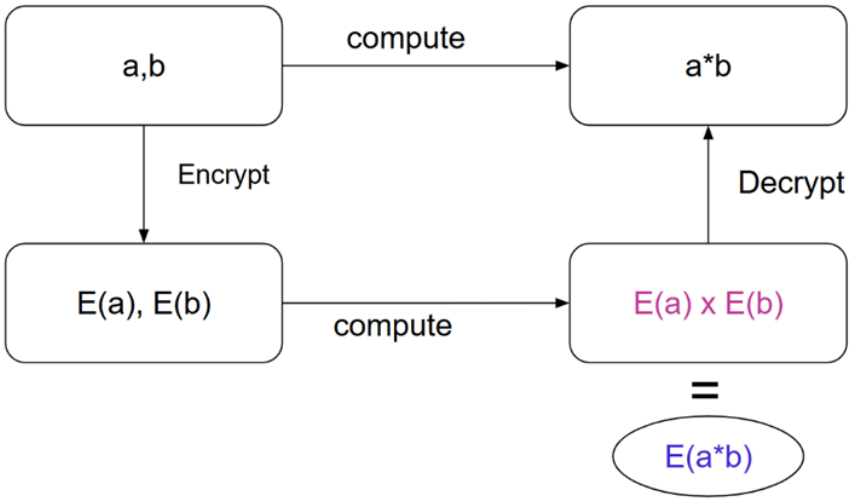
→ Solution: Homomorphic Encryption

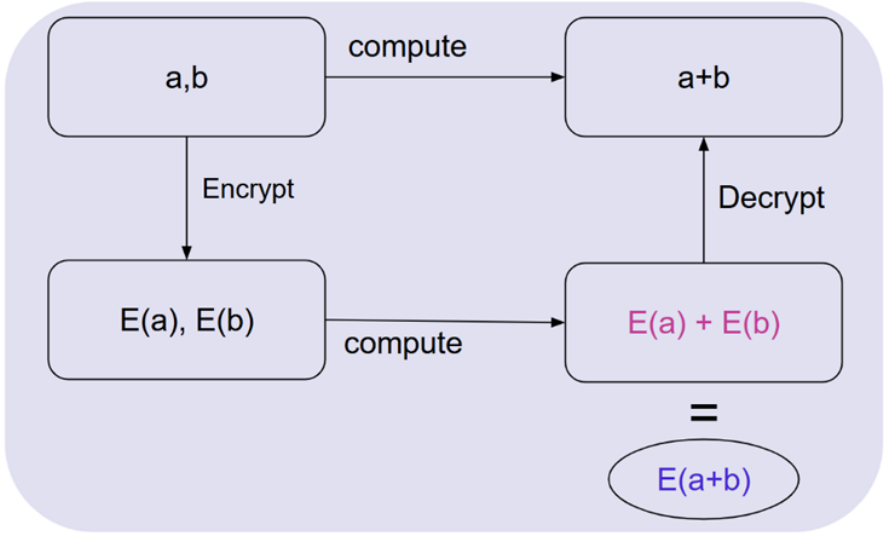
Data Protection 1-0-1



- Encryption Scheme: (Gen,Enc,Dec)
- Gen ⇒ (pk,sk)
- $Dec_{sk}(Enc_{pk}(m)) = m$

Homomorphic Encryption (HE)





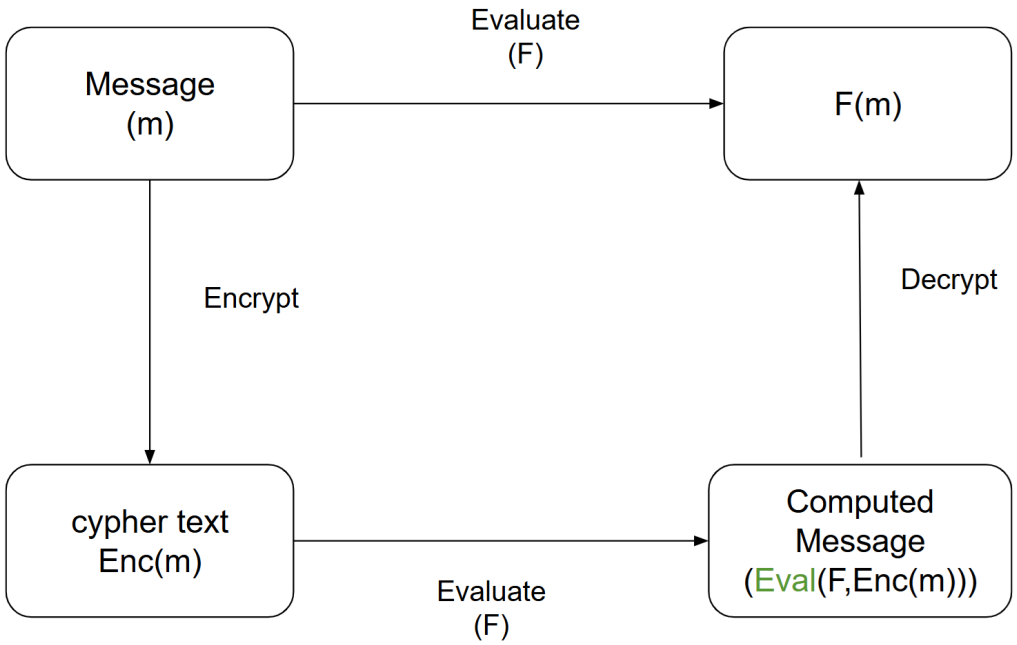
- Homomorphic encryption (HE) introduces evaluation over encrypted data
- Evaluation Operations = Multiplication, Additions, Polynomial

Homomorphic Encryption (HE)

- Homomorphic encryption (HE) introduce evaluation over encrypted data
- HE Scheme: (Gen,Enc,Dec,Eval)

Gen ⇒ (pk,sk)

$Dec_{sk}(Eval_{pk}(F,Enc_{pk}(m)) = F(m)$



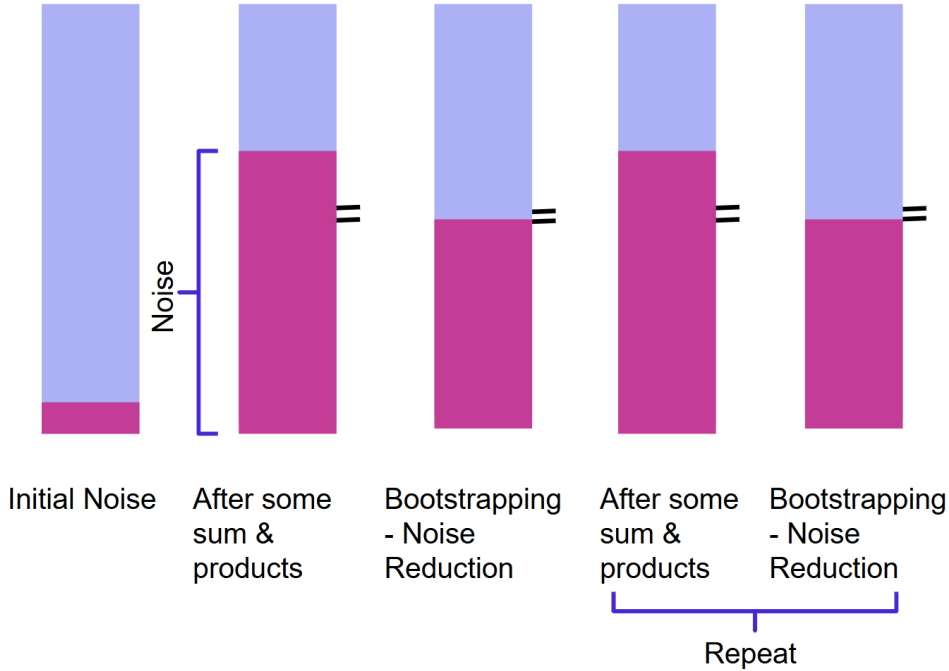
Homomorphic Encryption (HE) and Noise

- Noise is Critical for HE Security
- Noise grows with every operation.
- If noise grows beyond a threshold decryption will output incorrect bit.

- We can compute
  - Additions ⇒ many
  - Multiplications ⇒ few
- How to compute more !!

Gentry's blueprint : Bootstrapping

- Decryption eliminate the noise but insecure to provide secret key
- Solution : Homomorphically decrypt given $Enc_{pk}(sk)$
- Infinite number of evaluation operations possible with bootstrapping
- Bootstrapping - Computationally Expensive Operation



Noise

Homomorphic Encryption (HE) Types

Type	Characteristic
Partially Homomorphic Encryption (PHE)	Single Type of Operation (Addition or multiplication)
Somewhat Homomorphic Encryption (SHE)	Limited number of both Addition & Multiplication. Constraints on complexity of computation
Fully Homomorphic Encryption (FHE)	Unlimited number of both additions and multiplications

HE Schemes & Libraries

Binary Arithmetic Schemes	Exact Arithmetic Schemes	Approximate Arithmetic Schemes
• DM/CGGI (FHEW/TFHE) • Exact,Fast Bootstrapping, Single Bit operations • Scalability issues	• BGV/BFV • Operates on Integer vectors, most mature • Slow bootstrapping but high bandwidth	• Approximate, operates on real vectors • Faster than BGV/BFV but at cost of approximate results • Typical application : machine learning, statistics

- **Some Libraries**
  - OpenFHE , Lattigo, tfhe-rs, SEAL
  - Languages : C/C++, Python,GO,rust

RSAC 2025 Conference

Practical implementation and real-world applications of HE

Applications of Homomorphic Encryption (1)

- Secure Cloud Computing (Confidential outsourced Computation)
- Privacy-preserving machine learning (PPML)
- Privacy-Preserving Data Analytics
- Secure Data Sharing and Collaborative Secure Analysis
- Encrypted Searchable Databases
- Privacy preserving Healthcare Applications
- Secure/Confidential Financial Transactions
- Privacy-Preserving Biometric Authentication

Typical Applications Examples of HE

Secure Cloud Computing (Confidential Outsourced Computation) ★★★★★

Data Types: Financial records, proprietary algorithms, or sensitive personal data.

Real-World Use: Multiple Libraries like HElib and SEAL are already deployed for encrypted SQL queries and lightweight computations.

Challenges: Performance overhead for complex computations (e.g., deep neural networks).

Privacy-Preserving Healthcare Applications ★★★★★

Data Types: Medical imaging, genomic sequences, prescription histories.

Real-World Use: iDASH Competition projects use HE for genome-wide association studies (GWAS).

Challenges: Large datasets and complex computations strain performance.

Encrypted Searchable Databases ★★★☆☆

Data Types: Encrypted emails, legal documents.

Real-World Use: Niche uses in military/government sectors.

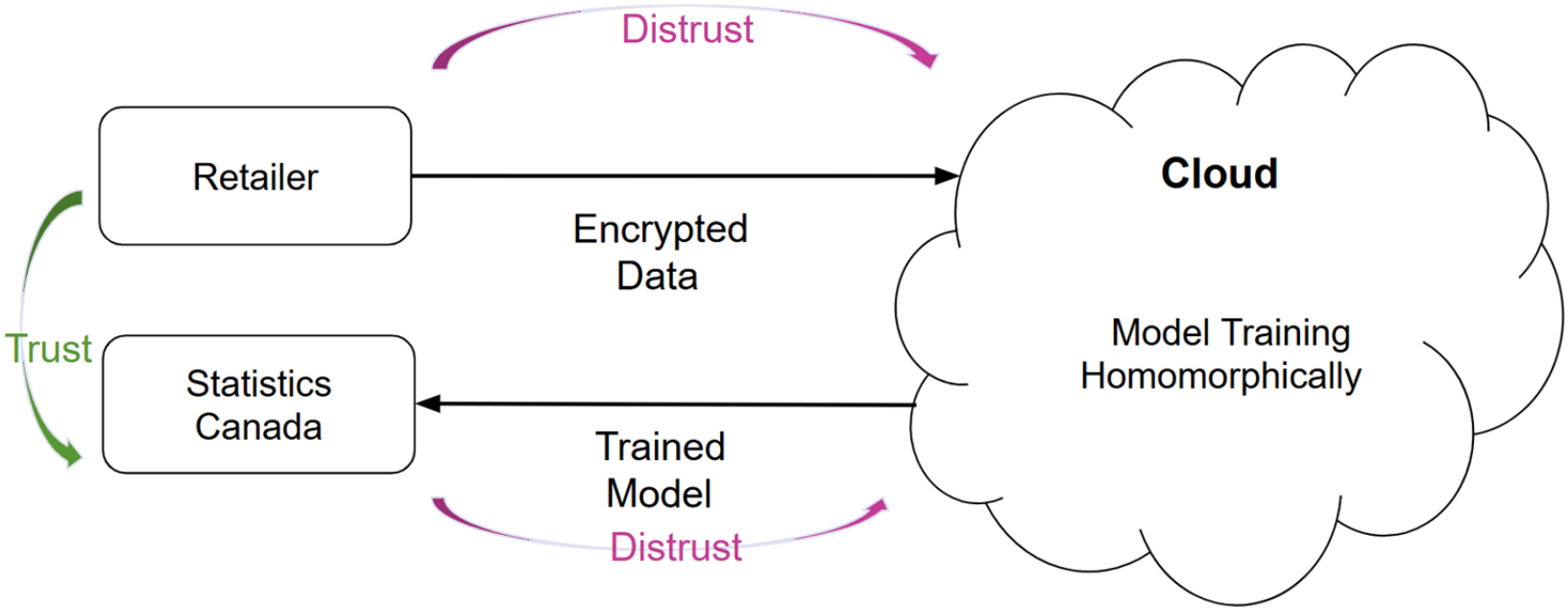
Challenges: High latency for large databases; simpler SSE schemes may often suffice.

★ Current HE Suitability

Statistics Canada : Training a machine learning model for text classification

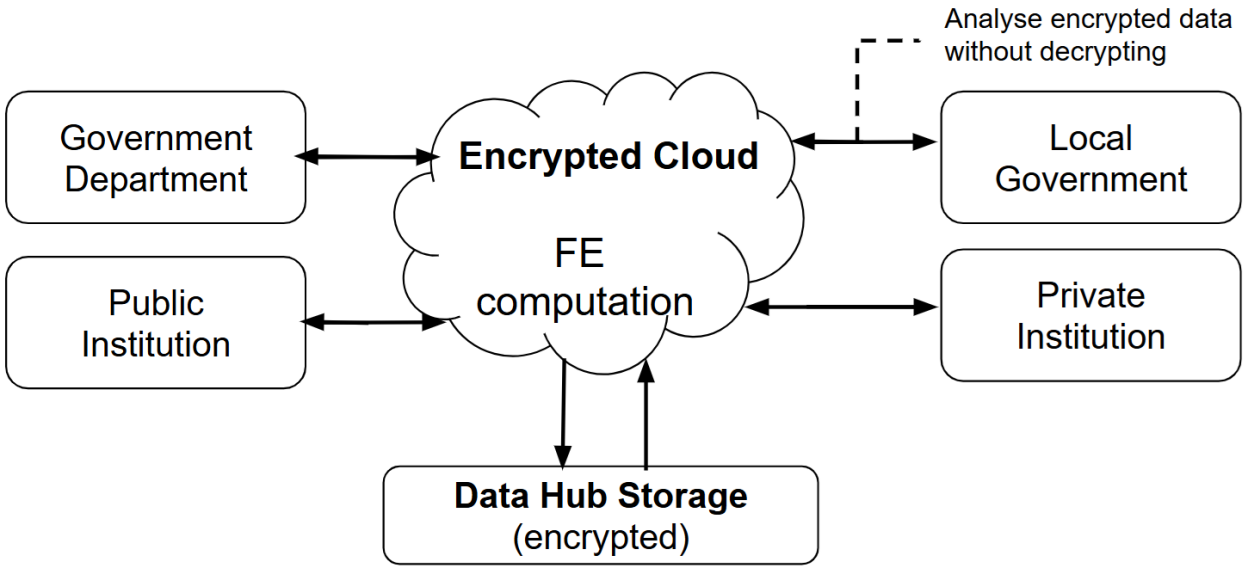
Privacy-preserving machine learning (PPML)

- Input data is encrypted and transferred to cloud environment for Homomorphic machine learning



Statistics Korea : Developing a Privacy Preserving statistical data hub platform

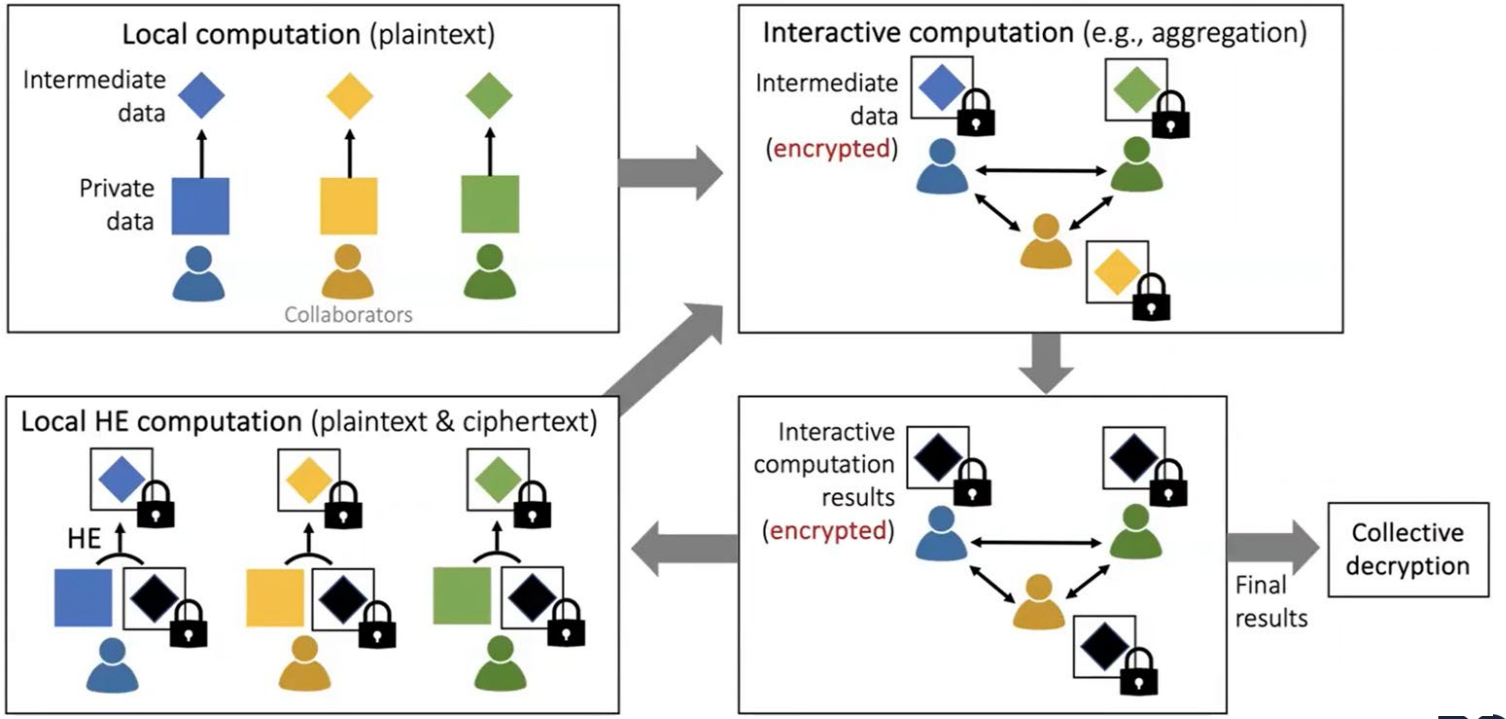
- **Datasets linked in their encrypted state, and two computations performed**
  - Generation of descriptive aggregate statistics related to shop space and turnover
  - Logistic regression to model the impact of the Covid-19 pandemic on small businesses.



Secure Genome-Wide Association Study(GWAS) on UK Biobank Dataset

Secure Data Sharing & Collaborative Analysis in Healthcare Application

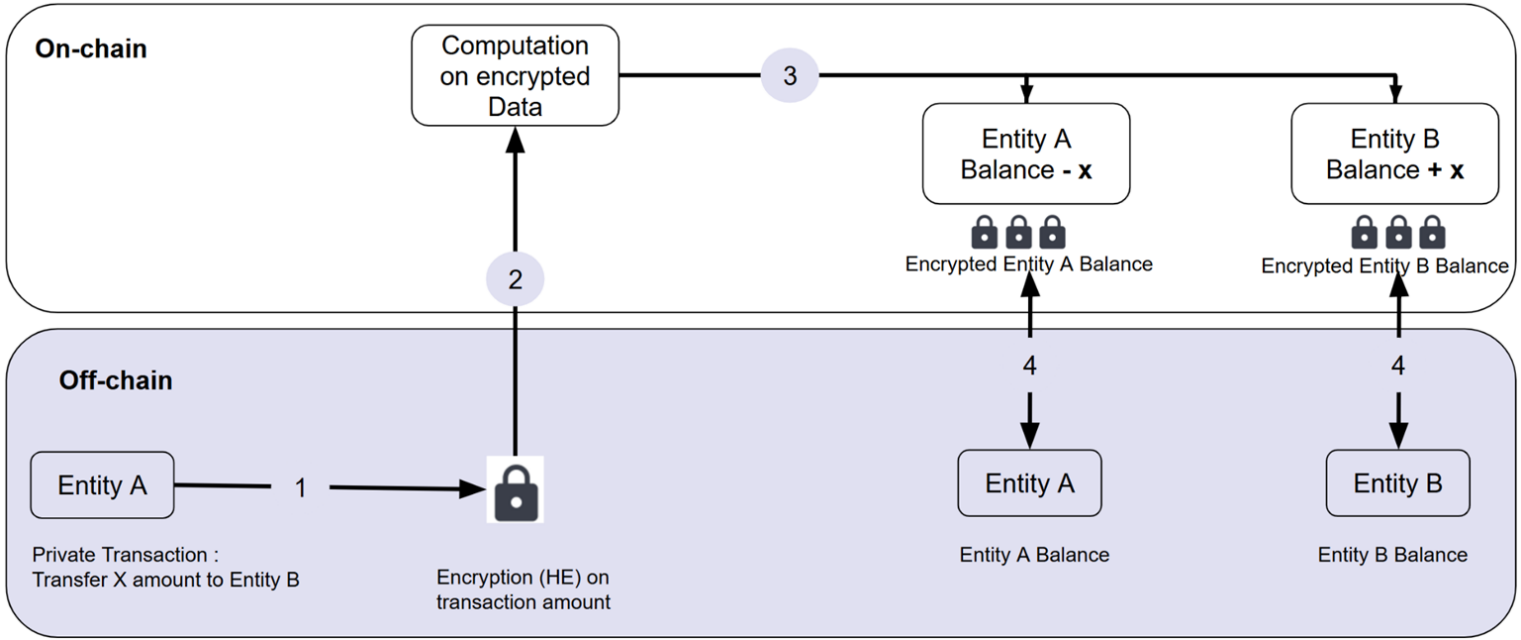
- Multiparty Homomorphic Encryption (MHE) enable Federated Secure computation



Blockchain : Transfer on-chain assets between entities using on-chain FHE to improve confidentiality

Secure/confidential Financial Transactions

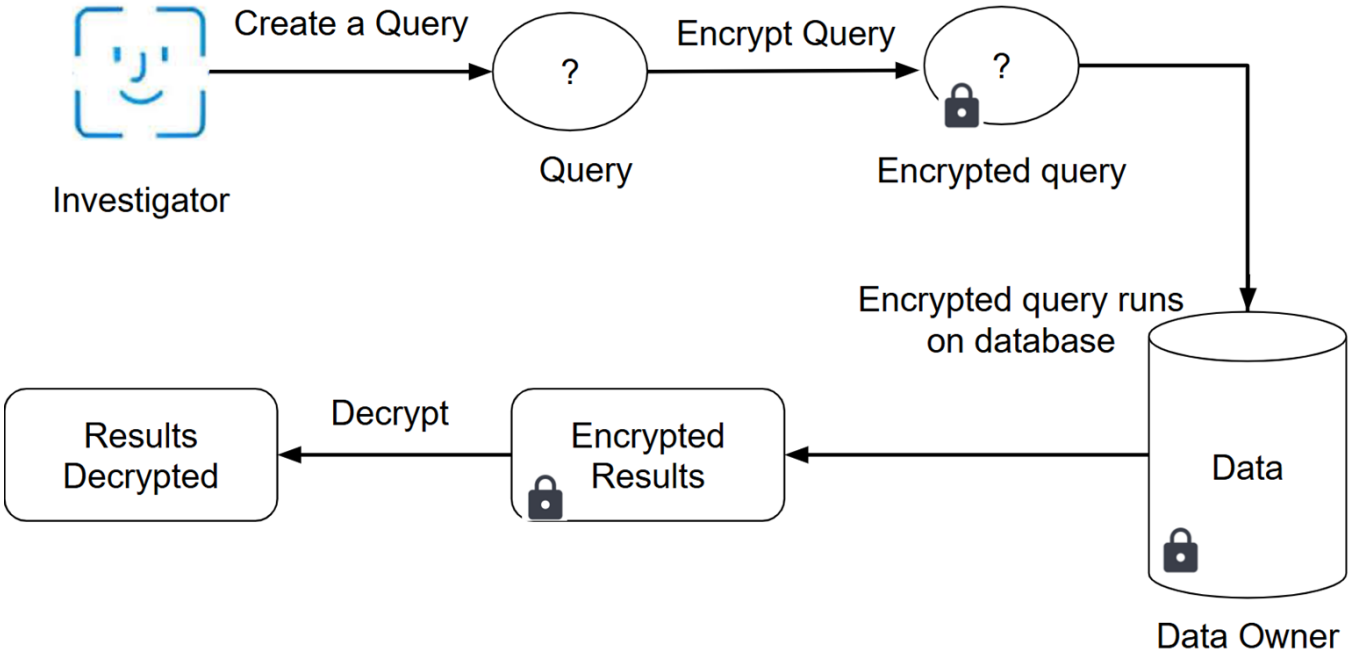
- FHE can address on-chain confidentiality by enabling verification without exposing sensitive data



Stock Exchange : Data Broker for government agencies using homomorphic encryption

Encrypted Queries/ Searchable Databases

- FHE-encrypted queries with encrypted analytics over data

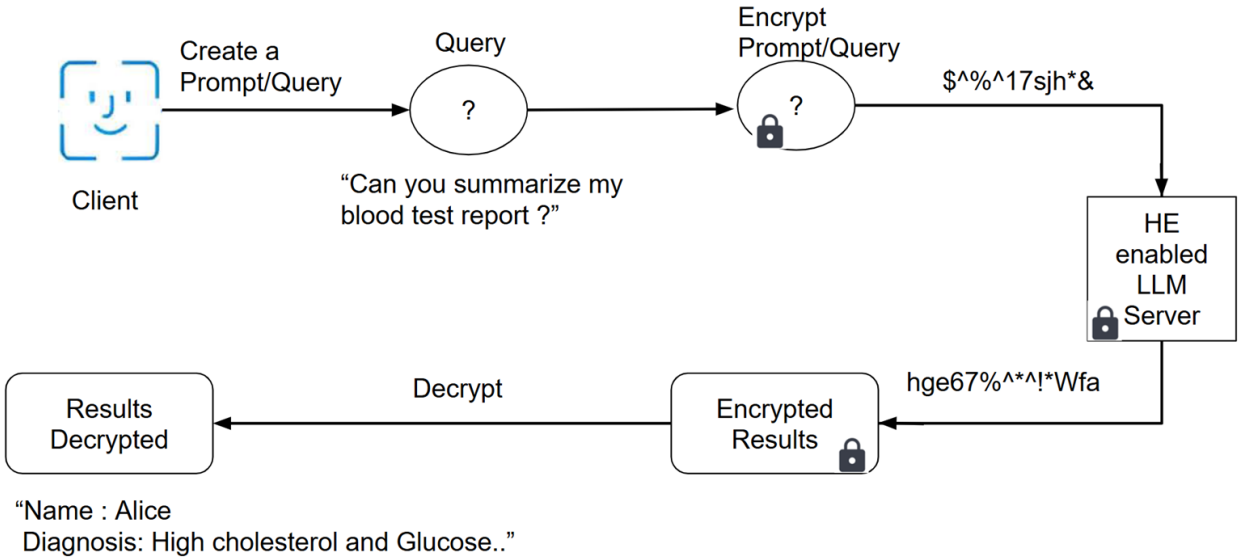


RSAC 2025 Conference

Large Language Model (LLM) Inference using Fully Homomorphic Encryption

Privacy-preserving machine learning (PPML)

- FHE-encrypted prompts to LLM for Non-real-time applications such as document summarization and fine-tuning models on private data
- GPU-based implementation of the transformer architecture using CKKS



RSAC | 2025 Conference

Homomorphic Encryption Challenges & Recent Advancements

Homomorphic Encryption Challenges

- Performance & Efficiency
- Implementation Complexity
- Noise Management
- Absence of Standardization
- Key Management

Recent Advancements

- Hardware Acceleration (GPU/FPGA/ASIC)
- Open-Source Ecosystem Growth, Software Libraries & Frameworks
- Hybrid HE-Secure Multi-Party Computation (MPC) Protocols
- NIST's HE Standardization Initiative

Optimized Schemes and Algorithms

- CKKS (Approximate Arithmetic)
- TFHE (Faster Bootstrapping)
- Sparse Homomorphic Encryption
- Post-Quantum HE Schemes
- Optimized Bootstrapping-Free HE

RSAC 2025 Conference

Homomorphic Encryption Security

Homomorphic Encryption Security (1)

Chosen Ciphertext Attacks

Operational Safeguards
Query Restriction
Differential Privacy
Zero Knowledge Proofs

Parameter Selection Vulnerabilities

Robust Parameterization
NIST standardized Parameters
lattice reduction advancements

Key Management Risks

Key Management Best Practices
Threshold cryptography
HSMs and key rotation

Side-Channel Attacks

Side-Channel Resistance
Hardware isolation
Secrets Splitting

Homomorphic Encryption Security (2)

Denial-of-Service Storage/bandwidth overheads

Ciphertext Optimization

Encoding/compression

Hardware acceleration

Post-Quantum Transition Uncertainties

Implementation Rigor

Open-source audits

Formal verification

RSAC 2025 Conference

Call for Action

Apply What You Have Learned Today (1)

- **Call to Action :**
  - *Start small, think big. Prioritize one use case, secure cross-functional buy-in, and build HE competency iteratively. The future of privacy-preserving compute is here—be its architect*

- **Next week you should :**
  - Assess HE Feasibility and Identify 1–2 high-value data workflows where encrypted computation could resolve privacy/regulatory hurdles.
  - Initiate Cross-Team Collaboration and align on HE's technical and regulatory requirements.

Apply What You Have Learned Today

- **In the first three months following this presentation you should :**
  - Launch a Pilot Project
  - Train Teams on HE Fundamentals
  - Adopt Scheme-Specific Best Practices
  - Optimize Performance

Tips for Pilot Project

- *“Small beginnings are the launching pad to great achievements”*
- Focus on small, structured Numerical datasets with linear workflows (e.g., summation, averaging), may be with Low Multiplicative Depth in high-compliance sectors
- Prioritize use cases where privacy justifies HE’s overhead, and pair HE with hardware acceleration or hybrid encryption models.
- Some challenging pilot projects examples include using Complex Unstructured Data, Complex Deep Learning, Real-Time Systems (eg high frequency trading) and very Large-Scale Datasets

Apply What You Have Learned Today

- **Within six months you should :**
  - Conduct Security Audits
  - Implement Governance Guardrails
  - Align with Regulatory Standards
  - Build HE Threat Models
  - Join HE Communities

RSAC | 2025 Conference

The future of privacy-preserving compute is here — be its architect

RSAC | 2025 Conference

Thank you

Deepak Behal
deepak.behal24@gmail.com